



Immediate Action Memorandum
from the
Federal Student Aid Chief Information Officer

September 14, 2006

Subject: Sensitive data protection on portable devices

As outlined in the Department of Education's Security Memorandum titled *Safeguarding of Personally Identifiable Information*¹: "In carrying out our mission, the Department of Education collects and maintains personal information on millions of students, their parents, grantees, employees and others. The recent major security breach at another agency highlights the importance of our duty to protect personal data from loss and misuse. ... Safeguarding personal information is an ongoing priority vital to maintaining the public trust."

In order to comply with this requirement, all Federal Student Aid staff and supporting contractors must take immediate action to ensure that the following policy is enforced to protect the sensitive information stored on all portable devices (laptops, flashdrives, CD/DVDs, tapes, cell phones, etc.)

This memorandum provides additional policy guidance and technical information to Federal Student Aid regarding protecting mobile data.

Policy:

All sensitive information (personally identifiable information², non-public financial information, and proprietary information) must be encrypted when stored on any portable device.

Effective Date: Immediate

Encryption requirements:

- Devices can use total drive, container/partition, or file-based encryption.
- Either hardware or software encryption is acceptable.

¹ This memorandum can be found at the following Department of Education URL:
<http://connected.ed.gov/index.cfm?articleobjectid=113476C0-0D99-F2A5-0CD25F34EAD358DA>

² For purposes of this policy, the term "personally identifiable information" means any information about an individual maintained by Federal Student Aid, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information with is linked or linkable to an individual.

- Encryption must use the AES encryption algorithm with a minimum key length of 128 bits.
- When an access password is required to encrypt or decrypt the information, the password must be 12 characters in length and use three of the following: Upper Case letter, Lower Case Letter, Number, Special Character. Passwords must be kept secret and not shared.

The Department of Education is currently in the process of identifying standard hardware and software for encryption on our portable devices. Federal Student Aid currently uses WinZip and TrueCrypt software for encrypting data on our portable devices and is in the process of purchasing encrypted flashdrives for specific users. However, the need for protecting our data on portable devices through encryption is immediate. Please use any interim method available that meets our encryption requirements.

If you have questions about whether a specific tool meets these criteria or need further information, please email Robert.Ingwatson@ed.gov.



Katie Blot
Chief Information Officer
Federal Student Aid